无线传感器网络云信任模型

马 彬 谢显中
(重庆邮电大学计算机科学与技术学院 重庆 400065) (重庆邮电大学个人通信研究所 重庆 400065)

摘 要 针对目前无线传感器网络不能有效降低信任风险的问题,提出一种用云理论定义的风险信号,并构建基于该风险评估方法的无线传感器网络云信任模型。该模型考虑到无线传感器网络中节点的动态上下文的不确定性,引入一种新的基于云理论的风险评估方法,并提出把风险和信任不确定性统一起来。实验结果分析表明,该信任模型能够有效表达信任和风险的不确定性,降低信任风险,相比已有的一些信任模型较大程度地降低了信任风险,提高了系统的有效成功合作率。

关键词 信任模型,风险,云模型
中图法分类号 TP393 **文献标识码** A

Cloud Trust Model for Wireless Sensor Networks

MA Bin XIE Xian-zhong
(School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)
(Institute of Personal Communications, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract In wireless sensor networks, it is difficult to take from the rate of trust risk. This paper used the concept or cloud theory to estimate dynamic context and consequently presented the definition of risk signal, and a cloud trust model based on risk evaluation for wireless sensor networks was proposed in this paper to solve this problem, in which the uncertainty between dynamic context relationships is considered. The risk was evaluated using cloud theory, quantified using risk and trust uncertainty degree presented in a uniform form. The simulation results show that the proposed trust model based on risk evaluation can efficiently express uncertainty of risk and trust, and decrease trust risk of nodes. And so this trust model also can evidently take from the rate of trust risk, and enhance successful cooperation ratio of system.

Keywords Trust model, Risk, Cloud model

1 引言

传统信任模型认为信任就是认证信任的实体和不信任的实体,并拒绝不信任实体的访问,是为了保证网络环境安全性的一种安全机制。借鉴人的信任认知行为学而产生的计算机信任模型近十年来得到了广泛和深入的研究。与信任认知行为学相似,信任模型中设定的信任不一定都无害,不信任也不一定都有害,仅凭信任-不信任界定无法有效保证系统安全。而且我们所能认识的信任实体和不信任实体只是整个信任问题中的一个子集。由此产生的将未知的信任实体当作不信任实体或未知的不信任实体当作信任实体来判定的现象,称之为伪判定。这种现象的存在导致信任存在一定的风险和系统有效成功合作率较低。

鉴于这些问题,国内外的学者都积极想办法解决。何锐[1]等将云模型引入到开放网络环境的信任模型研究中。云模型[2]是用语言值表示的某个定性概念与其定量表示之间的不确定性转换模型。它将模糊性和随机性结合起来,从而能够更好地对不确定性进行描述。作者认为不确定性是信任的重要属性,即实体之间的信任关系具有模糊性和随机性。基于此,提出了一种基于云理论的信任模型。该模型以云的形式,将实体之间的信任关系的信任程度描述和不确定性描述统一起来,并给出了信任云的传播和合并算法。

但是,对于用信任云描述无线传感器网络环境中实体之间的信任关系,存在的信任风险没有得到论述。而要解决信任风险问题,所要解决的第一重要问题就是什么是"信任风险"。信任的伪判定率较高是当前各种信任模型的一个弱点,本文加入风险理论的观点,改进基于云理论模型的信任模型,提出了基于信任风险和信任云的信任模型。对于风险理论应用于无线传感器网络环境中待解决的核心问题——"风险"的评估问题,本文也提出了自己的"风险"评估方法。

本文认为,"风险"由动态变化引起,任何一个系统(包括信任认知行为和计算机系统)在正常情况下,如果没有动态变

到稿日期:2009-05-25 返修日期:2009-08-17 本文受国家自然科学基金(60872037),重庆市教委科学研究计划(KJ090506),重庆邮电大学自然科学基金(A2008-48)资助。

马 彬(1978-),男,硕士,讲师,主要研究方向为信任管理、无线传感器网络,E-mail:mab_cqupt@sina.com;谢显中(1966-),男,博士,教授,主要研究方向为无线网络安全、感知无线电。

化产生，是不会有风险发生的。但这里所说的“动态变化”是个相对概念，本文认为，系统正常范围内的动态变化也属于“静止”，只有超过正常范围的动态变化才是真正的变化。因此，可以通过监视网络上下文信息的动态变化来感知风险。但动态变化到什么程度才被认为是“风险”，这个界限是不确定的，难以用一般的数学模型来描述，因此本文借鉴描述不确定性的工具——云模型来描述上下文信息的动态变化，从而定义“风险”的发生。

本文提出一种基于风险的无线传感器网络云信任模型。通过对各种上下文信息进行综合分析和识别风险，产生风险信号，从而开展对上下文信息的风险评估和量化，并依据风险值改进云信任模型，进而更加客观真实地反映实体的可信度，为系统进行安全决策提供依据。

本文第 2 节介绍相关研究；第 3 节论述风险的相关定义及评估方法；第 4 节介绍无线传感器网络云信任模型；第 5 节给出实验并分析测试结果；最后对全文进行总结。

2 相关研究

从社会学角度看，信任关系是一个很难度量的抽象的最复杂的社会关系之一，当实体之间的信任关系不能明确定义时，它也是不确定的，给它的评估和管理带来了难度。信任也是与上下文也相关的一个动态过程，随着时间的变化，实体之间的行为上下文可能会动态地变化。信任模型的研究主要集中在两个方面，即静态信任模型（早期信任模型）和动态信任模型。

信任管理（trust management）的概念首先由 Blaze[3] 等人提出，其基本思想就是承认系统中安全信息的不完整性，系统的安全决策需要依靠可信任第三方提供附加的安全信息。随后许多信任模型被提出，如 Josang 模型[4]、Beth 模型[5] 等。虽然这些模型提出了信任度量、信任推荐和传递、综合信任等功能，但信任动态性、信任不确定性和信任的防御性都没有体现。因此把这些信任模型称为静态信任模型。

近几年，一些学者开展了各种分布式应用中动态信任管理方面的研究工作。他们使用各种不同的数学方法和工具建立动态信任关系的模型，如 Tang 模型[6]、Chen 模型[7]、Tian 模型[8]、Hassan 模型[9]、Han 模型[10]、Sun 模型[11]、Dimitri 模型[12]、Yung 模型[13]、Liu 模型[14] 等，并取得了一些新的进展。这些模型虽然都考虑了信任关系的动态性、支持信任推理和更新、信任的模糊性、具备有限的防御能力等，但大部分模型都不支持信任风险的评估，不能真实有效地体现不确定网络环境中信任的不确定性。

据不确定网络环境的特性，系统安全决策应根据主观策略平衡风险和信任因素的结果作出，单纯动态信任模型或风险评估并不能解决系统安全决策问题。目前，对于信任和风险之间的关系的研究还很薄弱，Manchala[15] 最早探索信任和风险之间的关系，但是缺乏信任度量。Josang[16] 扩展了上述模型，阐述了信任和风险的关系，并分析了风险对于安全决策的作用。张润莲[17] 等人通过分析实体行为中潜在的风险对系统安全决策的影响来评估实体行为风险，并在此基础上计算实体的信任度。这些工作考虑了信任和风险之间的关系并进行了分析和评估，但是没能考虑信任风险本身存在的不确定性，不能客观、准确地描述实体之间信任风险的不确定性。

3 基于云模型的风险相关定义及评估方法

3.1 云理论模型

云模型主要反映宇宙中事物或人类知识中概念的两种不确定性：模糊性（边界的亦此亦彼性）和随机性（发生的概率），它把模糊性和随机性完全集成在一起，研究自然语言中最基本的语言值（又称语言原子）所蕴含的不确定性的普通规律，使得有可能从语言值表达式的定性信息中获得定量数据的范围和分布规律，也有可能把精确数值有效转换为恰当的定性语言值。

云是用语言值表示的某个定性概念与其定量表示之间的不确定性转换模型，用以反映知识中概念的不确定性。云由许许多多个云滴组成，一个云滴是定性概念在数量上的一次实现，单个云滴可能无足轻重，在不同时刻产生的云的细节可能不尽相同，但云的整体形状反映了定性概念的基本特征。云的“厚度”是不均匀的，腰部最分散，“厚度”最大，而顶部和底部汇聚性好，“厚度”小。云的“厚度”反映了确定度的随机性的大小，靠近概念中心或远离概念中心处确定度的随机性较小，而离概念中心不远不近的位置确定度的随机性大，这与人的主观感受相一致。

定义 1[2] 设 U 是一个用精确数值表示的定量论域（一维的、二维的或多维的），A 是对应于 U 空间上的定性概念，若定量值 $x \in U$，且定性概念 A 的一次随机实现，x 对 A 的确定度 $\mu(x) \in [0,1]$ 是有稳定倾向的随机数：

$$\mu: U \to [0,1] \quad \forall x \in U \; x \to \mu(x)$$

则 x 在论域中 U 上的分布称为云，每一个 x 称为一个云滴。

云的数字特征用期望值 Ex，熵 En，超熵 He 3 个数值表示。它们反映了定性概念整体上的定量特征。

期望 Ex（Expectation）：云滴在论域空间分布的期望。通俗地说，就是最能够代表定性概念的点。

熵 En（Entropy）：定性概念的不确定性度量，由概念的随机性和模糊性共同决定。

超熵 He（Hyper Entropy）：超熵是熵的不确定性的度量，即熵的熵。超熵越大，云滴离散度和确定度的随机性越大，云的“厚度”也越大。

正态云模型是在概率论的正态分布和模糊集合的隶属函数的基础上发展起来的全新模型。正态分布在理论和实际中应用非常广泛，但如果决定随机现象的因素单独作用不是均匀地小，相互之间并不独立，有一定程度的相互依赖，就不符合正态分布的产生条件，不能构成正态分布。正态云模型弱化了正态分布的前提条件，决定不确定现象的随机因素单独作用可以不是非常均匀地小；各因素相互之间可以不完全独立。这里用超熵衡量偏离正态分布的程度，将正态分布扩展为“泛正态”。在本文中使用的上下文信息和信任的动态变化满足“泛正态”的条件，可以用正态云模型描述。

正态云是最重要的云模型，正态云的期望曲线是一个正态型曲线。对于某一定性知识，其相应的云对应于 $Ex \pm 3En$ 之外的元素均可忽略。用正态云发生器算法实现从定性语言值到其定量表示之间的不确定转换，其具体算法[2] 为：

（1）生成以 En 为期望值、He 为标准差的一个正态随机数 Ex'；

（2）生成以 Ex 为期望值、En 的绝对值为标准差的一个

正态随机数 x，x 称为论域空间中的一个云滴；

(3)计算 $y=\exp[-(x-Ex)^2/2(En')^2]$；

(4)使(x,y)成为论域中的一个云滴；

(5)重复步骤(1)－步骤(4)直至产生 N 个云滴。

用该算法生成的云自然地具有不均匀厚度的特性，云的腰部、顶部、底部等并不需要精确地定义，3 个数字特征值足以很好地描述整个云的形态。

逆向云发生器的作用就是从一些给定的云滴中，求出表征云形态的 3 个数字特征值 Ex，En，He。逆向云发生器具体算法[2]如下：

输入：N 个云滴的定量值$[x_i]$；

输出：期望值 Ex，熵 En 和超熵 He；

(1) 计算云滴的均值 V，一阶矩 M_1 和二阶矩 M_2；

(2) $Ex=V$；

(3) $En=M_1\times\sqrt{\frac{\pi}{2}}$；

(4) $He=\sqrt{M_2-En^2}$。

3.2 风险的相关定义及评估方法

在无线传感器网络环境中，可以通过监视系统上下文信息的动态变化感知风险。且被监视的动态上下文信息往往不是连续可导的，即便是连续可导，其函数曲线也比较复杂，不便于用导数的形式描述。鉴于风险信号出现的不确定性，本文引入云模型来描述上下文信息的动态变化。在已知上下文的正常状态下用无确定度信息的逆向云算法绘制上下文正常状态云，并得到其数字特征。计算被监视时刻的上下文信息采样值的隶属度，若这一时刻的上下文信息采样值隶属于正常状态云，则认为没有风险产生，反之，则认为有风险信号产生。这样的描述更具有一般性。

定义 2 上下文信息云的定义 $Cloud=(I,t,Ex,En,He,\delta)$

其中，$I=\{S,E,C,R,U,\cdots\}$，I 代表被监视的上下文信息集合。

以 S 为例(以下均以 S 为例，其他上下文信息参照 S 描述)，$S=\{m_i\mid i=0,1,\cdots,n\}$，其中 m_i 表示以 t 为采样间隔时间所选取的 n 个空间信息(如位置信息)的采样点。

t：上下文信息的采样间隔时间。

Ex：以已知采样点为云滴，采用逆向云算法得出的上下文信息云的期望值，称之为云的重心。在这一点处，上下文信息肯定是正常的。计算式为：

$$Ex\approx\hat{Ex}=\overline{M}=\frac{1}{n}\sum_{i=1}^{n}m_i$$

En：以已知样本点为云滴，采用逆向云算法得出的上下文信息云的熵。熵的大小直接决定了在论域中可被模糊概念所接受的范围，即上下文信息可以被认为是正常的范围。计算式为：

$$En\approx\hat{En}=\sqrt{\frac{\pi}{2}}\times\frac{1}{n}\sum_{i=1}^{n}|m_i-\hat{Ex}|$$

He：以已知采样点为云滴，采用逆向云算法得到的上下文信息云超熵。计算式为：

$$He\approx\hat{He}=\sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(m_i-\overline{M})^2-\hat{En}^2}$$

δ：隶属度的阈值，通过实验观察和主体安全级别(也可是实体对象的重要性级别)由人工动态设置。

定义 3 上下文信息云的隶属度函数定义，设 m 为某一时刻 T 上下文信息 S 的采样值，由式(1)计算出 m 可以被认为是正常的确定度 μ：

$$\mu=e^{-\frac{(m-Ex)^2}{2(En)^2}}\tag{1}$$

$\mu>\delta$：T 时刻的上下文信息值属正常范围，无风险信号产生；

$\mu<\delta$：T 时刻的上下文信息值不属于正常范围，有风险信号产生。

这里定义的风险信号都是基于单个上下文信息的，仅凭一个上下文信息产生的风险信号不足以断定“风险”的发生，需要综合多种上下文信息的风险信号综合判断。本文给出了“风险”的评估方法。

定义 4 “风险”的定义：

$Risk=(I',Q,\varphi)$，其中，$Risk$ 是风险信号的综合加权程度，即风险值(或风险度)。

I'的含义为 I 上下文信息集合对应的风险信号。

$Q=\{q_1,q_2,\cdots,q_n\mid 0<q_i<1\}$：代表每一种上下文信息风险信号在整个系统的“风险”判定中所占的权重。

φ：判定“风险”的阈值，超过这一阈值，认为有风险发生。

$Risk=S'\times q_1+E'\times q_2+C'\times q_3+R'\times q_4+\cdots>\varphi$：有风险发生；

$Risk=S'\times q_1+E'\times q_2+C'\times q_3+R'\times q_4+\cdots\leqslant\varphi$：上下文正常，无风险发生。

4 无线传感器网络云信任模型

我们认为风险是动态变化产生的有用信息，应该结合到信任模型中。故改进了何锐等提出的基于云模型的信任管理模型。

4.1 基于风险的信任云定义

信任云是本模型的核心概念。借鉴云的形式化定义给出其形式化定义如下。

定义 5 信任云是以二维正态云的形式来描述节点之间的信任关系，其表述为：

$$\left.\begin{aligned}&tc_{AB}=nc(Ex,En,He,Risk)\\&0\leqslant Ex\leqslant 1,0\leqslant En\leqslant 1\\&0\leqslant He\leqslant 1,0\leqslant Risk\leqslant 1\end{aligned}\right\}$$

即节点之间的信任是一个正态云，其中，Ex 是信任期望。它表明了节点 A 对 B 的基本信任度；En 是信任熵，反映了信任关系的不确定性；而 He 是信任超熵，反映了信任熵的不确定性；$Risk$ 是信任风险，反映了信任的风险程度。

4.2 信任传播

在无线传感器网络环境中，节点不能总直接从相邻节点处获得陌生节点的推荐信任值，因此引入信任传播。假设有 m 个节点 $E_1,E_2,E_3,\cdots,E_m$，节点 E_i 和 $E_{i+1}(0\leqslant i\leqslant m-1)$存在信任云 $tc_i(Ex_i,En_i,He_i,Risk_i)$，这时，常常需要据此计算 E_1 对于 E_m 的信任云 $tc(Ex,En,He,Risk)$。

由于 E_1 对于 E_m 的信任云是通过中间节点传递的，因此把这叫做信任云的传播，其计算算法如下：

$$\left.\begin{aligned} tc(Ex,En,He,Risk)=tc_1\otimes tc_2\otimes\cdots\otimes tc_m=\\ \prod_{i=1}^{m}tc_i(Ex_i,En_i,He_i,Risk_i)\\ Ex=\prod_{i=1}^{m}Ex_i,En=\min(\sqrt{\sum_{i=1}^{m}En_i^2},1)\\ He=\min(\sum_{i=1}^{m}He_i,1),Risk=\min(\sum_{i=1}^{m}Risk_i,1) \end{aligned}\right\}$$

其中，⊗被称作信任云逻辑乘计算符。通过对参数意义的分析可知，信任云的期望更加趋近 0，超熵即云滴的离散度增加，显然经过传播以后，信任云的信任程度减小，不确定性和风险性增加，这符合实际情况。

4.3 信任合并

在无线传感器网络环境中，众多节点间信任关系构成了一个信任网络，两个节点之间常常存在多条信任路径。这样，在计算两个节点的信任关系时根据不同的信任路径就会得到多个信任云。这时，就需要将这些信任云合并成一个信任云。

假设存在 m 个信任云 $tc_1,tc_2,tc_3,\cdots,tc_m$，则它们可以根据下面的算法合并成一个信任云 $tc(Ex,En,He,Risk)$：

$$\left.\begin{aligned} tc(Ex,En,He,Risk)=tc_1\oplus tc_2\oplus\cdots\oplus tc_m=\\ \sum_{i=1}^{m}tc_i(Ex_i,En_i,He_i,Risk_i)\\ Ex=\frac{1}{m}\prod_{i=1}^{m}Ex_i,En=\min(\frac{1}{m}\sum_{i=1}^{m}En_i,1)\\ He=\min(\frac{1}{m}\sum_{i=1}^{m}He_i,1),Risk=\min(\frac{1}{m}\sum_{i=1}^{m}Risk_i,1) \end{aligned}\right\}$$

其中，⊕被称作信任云逻辑加计算符。通过对参数意义的分析可知，合并信任云的信任程度、不确定性和风险性方面都要优于前两种信任云。

5 实验及结果分析

基于仿真平台 Repast 模拟了一个基于开放 WSN 网络的实体协同服务环境。在该平台上，实现了改进 Cloud 信任模型（基于云理论）以及另外 3 个作为对比的信任模型，即 Chen 信任模型（基于证据理论）、Beth 信任模型（基于概率论）和 Tang 信任模型（基于模糊逻辑）。

5.1 实验环境及评价指标

5.1.1 实验环境

假设网络是完全开放分布式的，不存在统一的信任评估中心，实体只能通过自己的直接经验或推荐经验来度量请求实体的信任程度。在实验中，用仿真工具模拟了一个 WSN 开放网络环境，在有限空间环境中放置了一些实体，实体之间是可以直接进行交互的。网络环境中提出服务请求的服务请求实体向服务提供实体提出交互请求，可能被请求提供信任推荐的实体称为推荐实体。环境中上述 3 类实体都是可以随机选取的，且实体之间的信任关系也是随机产生并初始化的。

在实验中，指定 WSN 开放网络环境中实体之间总的交互次数。在每次交互中，仿真模型将随机选择网络环境中的两个实体，第一个实体是请求服务实体，另外一个为服务提供实体。服务提供实体将用改进信任云模型计算请求实体的信任程度，并且通过比较评估信任结果与初始的信任阈值，决策是否接收请求，且重要上下文信息将被反馈给相应管理器。

在实验前，需要对网络中的许多环境参数进行初始化，以便能够在相同的实验初始条件下对几个信任模型进行比较实验研究。实验的环境参数如表 1 所列。

表 1 实验环境参数及初始值

参数	值
初始信任实体数	8
实体通信距离	20
网络拓扑数	100
交互数	1500
信任阈值	0.5
实体数目	100
网络空间范围	250×250
伪判定概率	0.25

各参数具体说明如下：

初始信任实体数：实验开始时每个实体所拥有的可信任实体的数目，该参数可动态改变；

实体通信距离：实体间进行直接通信的最大距离。该处的距离是一个逻辑概念，实际可能是无线通信的覆盖范围；

网络拓扑数：由于在 WSN 开放网络中实体可移动，因此将整个实验过程分成很多次，每次具有不同的网络拓扑。但每次的实体及其信任关系都是延续的，只是改变了位置而已；

交互数：每一次实验中，实体（随机选取）间进行交互的总数；

信任阈值：实体预先设置的信任值，可决定实体不同的信任接受程度，并作出相应的信任决策；

实体数目：实验中实体的总数；

网络空间范围：实体所在的空间大小；

伪判定概率：实验中可能出现伪判定实体的比例。

5.1.2 实验评价指标

由于在真正的 WSN 开放网络环境中，不是所有的实体都能准确地被判定为信任或不信任，因此，在实验中定义了一个伪判定概率，它描述了一个实体作出信任某实体而被欺骗和可信实体被拒绝的概率。主要针对 CTMRE 系统的两个主要的功能进行测试分析，第一是测试其网络平均信任风险密度，即整个网络环境的交互风险水平；第二是测试系统有效规避伪判定，提供服务的有效成功合作程度。因而，定义了两个实验指标。

定义 6 若网络环境中所有实体的集合为 $E=\{e_i\mid 1\leqslant i\leqslant N\}$，实体间所有信任风险的集合为 $V=\{(e_i,e_j,r_{ij})\mid e_i,e_j\in E,0<r_{ij}\leqslant 1\}$，则平均信任风险密度为：

$$\rho_v=\frac{\sum\limits_{r_{ij}\in V}r_{ij}}{P_N^2}=\frac{\sum\limits_{r_{ij}\in V}r_{ij}}{N\cdot(N-1)}$$

它反映了整个网络的信任风险程度。

定义 7 若一定时期内网络中所有实体的交互次数为 N，其中合作的总次数为 M，伪判定合作次数为 P，则定义有效合作成功率为：$\theta=\frac{M-P}{N}\times 100\%$，它显示了网络中实体间的有效成功合作程度。

5.2 仿真结果分析

经过实验，网络的平均信任风险密度如图 1 所示。从图可知，Cloud 信任模型的平均信任风险低于另外 3 个模型，且 3 个信任模型的平均信任风险密度非常的接近。所以在一定风险情况下，Cloud 信任模型能够提高 WSN 开放网络环境中实体之间的成功合作可信水平。

有效合作成功率的实验结果如图 2 所示，从图可知，Cloud 信任模型的合作成功率显著地高于另外 3 个，使得另外两个模型的曲线极其接近，以至于 Beth 信任模型的曲线被

Chen信任模型所覆盖。这主要是因为它引入了不确定性的原因。它不会因为不知道而拒绝，因此给大多数诚实的实体提供了更多的合作机会，从而提高了网络的合作成功率。

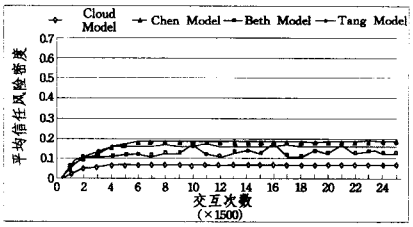

图1 平均信任风险密度实验结果

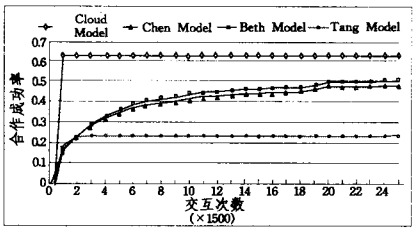

图2 合作成功率实验分析

结束语 本文从风险是由动态变化产生的这一角度，定义了无线传感器网络环境中的“风险信号”，进而定义了什么是“风险”。为降低无线传感器网络环境中的伪判定率，提出了新的风险信号评估方法，并改进了云信任模型。在对风险信号的评估中，鉴于上下文信息异常出现的不确定性，借用云模型理论来判定风险信号的发生。

在用多种不同上下文信息的动态变化来共同决定“风险”的发生这一问题上，本文提出的乘权重相加的方法，实际上没有考虑不同上下文信息之间动态变化的关联性。如果采用多维云模型来描述上下文的动态变化，将每个上下文信息作为云滴的一维，将更能反映问题的本质；同时在判断信任风险的过程中如何结合信誉的问题，这些都将是我们在未来一段时间所要做的工作。

参考文献

[1] 何锐，牛建伟，胡建平. 一种开放网络环境中的不确定信任模型[J]. 北京航空航天大学学报，2004，30(11)：1125-1128

[2] 李德毅，杜鹢. 不确定性人工智能[M]. 北京：国防工业出版社，2005

[3] Blaze M, Feigenbaum J, Lacy J. Decentralized trust management [C]// the Proceedings of the IEEE Symposium on Security and Privacy. USA: IEEE Computer Society Press, 1996: 164-173

[4] Josang A. The right type of trust for distributed systems[C]// Proceedings of the 1996 New Security Paradigms Workshop. California, USA, 1996: 119-132

[5] Beth T, Borcherding M, Klein B. Valuation of trust in open networks[C] // Proc. of the Conf. on Computer Security. New York: Springer-Verlag, 1994: 3-18

[6] 唐文，陈钟. 基于模糊集合理论的主观信任管理模型研究[J]. 软件学报，2003，14(8)：1401-1408

[7] Chen Haiguang, Wu Huafeng, Zhou Xi, et al. Reputation-based Trust in Wireless Sensor Networks[C]// Proc. of International Conference on Multimedia and Ubiquitous Engineering (MUE'07). 2007: 603-607

[8] 田春岐，邹仕洪，王文东，等. 一种新的基于改进型D-S证据理论的P2P信任模型[J]. 电子与信息学报，2008，30(6)：1480-1484

[9] Jameel H, Hung L X, Kalim U, et al. A trust model for ubiquitous systems based on vectors of trust values[C]// Proc. of the 7th IEEE Int'l Symp. on Multimedia. Washington: IEEE Computer Society Press, 2005: 674-679

[10] Han Guangjie, Choi D, Lim W. A Reliable Approach of Establishing Trust for Wireless Sensor Networks[C]// Proc. 2007 IFIP International Conference on Network and Parallel Computing. 2007: 232-237

[11] Sun Yan, Han Zhu, Liu K J R. Defense of Trust Management Vulnerabilities in Distributed Networks[J]. IEEE Communications Magazine, Feature Topic on Security in Mobile Ad Hoc and Sensor Networks, 2008, 46(2): 112-119

[12] Melaye D, Demazeau Y. Bayesian dynamic trust model[C]// LNCS 3690. Berlin: Springer-Verlag, 2005: 480-489

[13] Kyung T, Seo H S. A trust Model using Fuzzy Logic in Wireless Sensor Network[J]. Proc. of World Academy of Science, Engineering and Technology, 2008, 32(8): 69-72

[14] Liu Ke, Nael A-G, Kang K-D. Location verification and trust management for resilient geographic routing[J]. Journal of Parallel and Distributed Computing, 2007, 67(3): 215-228

[15] Manchala D W. Trust Metrics, Models and protocols for electronic commerce transactions[C]// Proc. of the 18th International Conference on Distributed Computing Systems. Washington, DC, USA: IEEE Computer Society, 1998: 312-321

[16] Josang A, Presti S. Analysing the relationship between risk and trust[C]// Proc. of the iTrust'04. LNCS 2995. Oxford, UK, 2004: 135-145

[17] 张润莲，武小年，周胜源，等. 一种基于实体行为风险评估的信任模型[J]. 计算机学报，2009，32(4)：688-698

(上接第78页)

[2] 王敏毅. 面向移动计算环境的分布对象技术[D]. 成都：电子科技大学，2002

[3] Capra L, Emmerich W, Mascolo C. Middleware for Mobile Computing[R]. UCL Research Note RN/30/01. Submitted for publication, July 2001

[4] Baggio A. Adaptable and Mobile-aware Distributed Objects[M]. Université Pierre & Marie Curie, June 1999

[5] Chen Guanling, Kotz D. A Survey of Context-aware Mobile Computing Research[R]. Dartmouth Computer Science TR2000-381. 2000

[6] Satyanarayanan M. Fundamental Challenges in Mobile Computing[C]// Proceedings of ACM PODC'96. 1996

[7] Noble B D, Satyanarayanan M, et al. Agile application-aware adaptation for mobility[J]. ACM SIGOPS Operating System Review, 1997, 31(5): 276-287

[8] Davis N, Friday A, Wade S, et al. A distributed systems platform for mobile computing[J]. Mobile Network Application, 1998, 3(2): 143-156